



What Broad Security Challenges May Canada Face by 2015?

By Jack E. Smith¹

Introduction

In November 2005, the Science & Technology Foresight Directorate of the Office of the National Science Advisor (ONSA) was asked to assist the new Public Security Technical Program (PSTP), a joint security technology initiative of Public Safety and Emergency Preparedness Canada (PSEPC) and Defence Research & Development Canada (DRDC).

The ONSA was asked to provide advice within the PSTP on a futures-oriented Public Security Science and Technology (PSST) agenda that could be aligned with the US Department of Homeland Security (DHS) as part of the Security and Prosperity Partnership of North America. It would also provide focus to the capabilities and skill areas that a new DRDC Centre for Security Science (CSS) might need to have to face the anticipated national security- all hazards challenges of the next decade.

ONSA's national security foresight experience is based upon its role as Canadian government partner in the US initiated Proteus² security foresight scenarios and Critical Thinking Game. We have been developing a foresight expertise through a series of collaborative projects aimed at emerging and frontier technology domains that will be relevant to national policy development in the next decade and beyond. These projects have involved several partners, mostly from inside the federal government, and have addressed subjects such as future fuels, bio-health innovation, geo-strategic systems, and animal health and infectious disease.³

Foresight⁴ is a process that relies upon a set of tools that encourages experts to extend their knowledge and vision through environmental scanning, technology roadmaps, scenarios and expert panels asking: *what if, and what prospective impacts?*

¹ Jack E. Smith is Director of S&T Foresight, for the Office of the National Science Advisor, (ONSA) Government of Canada. ONSA is located at Industry Canada and provides national S&T advice to Ministers and leads collaborative foresight studies in areas of national policy and science futures.

² Proteus is a national security foresight partnership of US and Canadian organizations involved in military and intelligence analysis, gaming and scenarios. See websites: www.carlisle.army.mil/proteus; www.proteuscanada.org;

³ Most of these studies are either unpublished or available from sponsors who collaborated with ONSA. Contact: Smith.Jack@IC.GC.CA for additional information

⁴ The Science and Technology Foresight Directorate (STFD) of the Office of the National Science Advisor (ONSA) manages technology foresight exercises and produces reports for the benefit of sponsors, participants and professionals interested in how emerging and prospective developments in global science and technology might impact the future in Canada, North America and the world. Foresight is the property of those who participated in the processes described herein, and therefore reflects the combined views of the participants. ***This work is undertaken under the leadership of the Government of Canada, but does not signify endorsement by its Departments and Agencies unless so indicated.***

Since we cannot predict the future, the approach is based upon contingent examination of several types of potential “future-shaping” factors, forces and their S&T linkages to the extent that these can be anticipated from the state of known or currently emerging science and technologies from research or underway at early stages of development. The intent is neither to be prescriptive, nor to identify a single forecast, but to create multiple, plausible alternatives that will represent a reasonable range of the situations for which we may have to be prepared in a rapidly changing world where S&T is usually a key driver.

When the DRDC-PSEPC team approached us in November 2005, our response was to create a network of broad security stakeholders⁵ and future S&T thinkers to reflect upon the key issues and questions outlined below. The remainder of this article will focus on the results of the broad risk-threat areas⁶ examined by this network.

The Protective Futures Workshop

The workshop was held on 26-28 March 2006 at DRDC Shirley’s Bay facility Ottawa. The workshop was organized to generate foresight that would feed into “Vision 2015” for the Systems Integration, Standards and Analysis (SISA) mission area of the Public Security Technical Program (PSTP) - a joint initiative of PSEPC and DRDC with the US Department of Homeland Security.

"Vision 2015" is the forward-looking framework to provide a perspective for the federal public safety and security community. It defines possible future challenges to public safety and national security in the 2015 timeframe, targets national capabilities for meeting those projected challenges, and provides opportunities available to science and technology for obtaining the identified capabilities. This necessarily includes a projection of capabilities for 'all-hazards preparedness' for the *future security of Canada's borders, the flow of people and goods across these borders, and for secure trans-border critical infrastructure*, as called for by the "Smart Border Declaration" and the "Security and Prosperity Partnership of North America".

Critical outcomes that the PSTP is directed to achieve include:

- Public safety and security policy to enable our national capability to be optimized; National emergency management system that ensures that capability is in place and responsive;
- Robust national surveillance and intelligence gathering and analysis that supports rapid intervention;
- Rapid identification of critical infrastructure vulnerabilities that can be mitigated to achieve enhanced all-hazards robustness

⁵ Some 30 + national security, university and foresight organizations participated in the workshop.

⁶ This article summarizes some of the key themes explored by the Workshop regarding broad risks, threats and vulnerabilities. The discussions about scenarios used to stimulate discussion, response capabilities and future S&T skill and technology needs are being left to a possible second article in a future edition of *Frontline*.

- National capabilities that ensure the safe, secure and efficient flow of people, goods and services across borders

Scanning and Risks - Key Answers to Hard Questions

Q1. What sort of world could we expect to see in terms of both major global and North American societal and technological *trends* and potential *discontinuities*?

Q2. What are the likely *risks* related to borders, infrastructure, and public security and safety more generally that will characterize 2015? These should include human-made and natural threats, hazards and vulnerabilities.

Workshop participants were provided with a “strategic environmental scan” based upon a wealth of expert information from national and international S&T specialists, security and intelligence focused professionals, and futures-technology and foreign-affairs generalists.

The discussion focused both on projected and plausible terror threats (divided opinions about probability and impacts) and on topics such as peak oil and transition to more sustainable fuels by 2015. No consensus was achieved, but evident trends became obvious in respect of more renewable and natural gas-unconventional hydrocarbon fuels from gas hydrates and other new sources, and on the growth of production and trade involving leading technologies by China and India.

Many felt that while the changes would be very significant for technology development, (quantum, cyber, nano, bio-info and convergent systems advances), trade would still be led and essentially determined by US-EU consumption patterns and the US primary trading partners at least until 2015. Central to the “all-hazards” and broad view of national security is the notion that relative security must be found at all levels of society – from individuals’ personal safety to societal freedom from arbitrary violence and individual rights infringements by the state. Many also indicated that new S&T innovations can be used to increase capabilities for both protection and enhanced threats – for example, the internet and its easily available “how to” guides, or should quantum computing become available before 2020, the first nation to acquire this capability will have an enormous intelligence advantage. Also nano-technology and its convergence with bio and info technologies may have both positive and negative implications.

Many of the most severe potential threats – such as deployment of weapons of mass destruction, intentional environmental or bio-food system terrorism were not seen as high probability for Canada although they might be used against the US. Their impact however would be very significant.

The Workshop concluded that the complexity of the security environment is likely to continue to increase with advances in S&T – since many of these raise issues of ethical choice about surveillance, and consent.

Clearly, the threat from global terrorism remains significant in the estimation of this group of foresight participants, but certainly not the only big challenge when a broad security definition is included.

From the perspective of many of the participants, terrorism represents a shock type of event - very high impact, but uncertain probability, and likely quite dependent on the depth and duration of Canada's global military alliances, deployments and commitments.

Table 1. A Sampling of Foresight Derived Public Security Threats, Risks and Vulnerabilities (various observations selected from the foresight discussions)	
•	Canada becomes fully technologically reliant on another country (e.g. USA) with a loss of independent capacity for risk readiness and detection
•	We have not developed defence capability against a full range of threats – so we accept a vulnerability, or at least lose time and scope for action in seeking the advice, guidance and protection of others in threat situations
•	Limited international collaboration – weakened intelligence, second rate technology and insufficient preparations to enable adaptive response capacities by national and responder level authorities – especially to a deployment of bio-terrorism or weapons of mass destruction.
•	Physical separation/geography does not protect us anymore in an asymmetric, digital warfare, global landscape threat environment
•	Government infrastructure may be more vulnerable than of the private sector with fewer direct stewards, lower capacity or outdated technologies
•	Environmental refugees could seek out Canada or we could be the source
•	Common global language could change from English i.e. to Chinese
•	We are not culturally educated enough for the 'global world'
•	Global warming leads to 'inevitable surprise' as diseases spread to newly warmed zones where insufficient readiness enables rampant spread
•	Lack of 'surge capacity' to respond to threats – from public authorities being ill equipped or not well organized and managed for threat management and mitigation
•	Over-harvesting of renewable resources could create dislocations of higher magnitude than in nations with less resource dependency
•	Urgent need for an Arctic strategy (opening of North-West Passage) as melting opens the possibility of year round sea lanes
•	Permafrost melts – making settlements unviable that have had ensured sovereignty from 1867- to present
•	Interoperability of command and control in an all-hazards environment – little experience and few rehearsals to enable efficiencies and standardize response protocols
•	Availability of weapons (information) on the internet – growing much faster than our ability to intercede maybe even track and analyze

- | |
|---|
| <ul style="list-style-type: none">• Human performance enhancement – an important new area of security towards which we have devoted almost no resources |
| <ul style="list-style-type: none">• Mobilized moral outrage - tipping point reached by disenfranchised youth – a potential consequence of multiculturalism gone awry if economic opportunities become closed to maturing youths, particularly those prone to extremist influences, now readily accessible on the internet |

Conclusion

The Workshop's proceedings themselves are expected to be of immediate interest to PSEPC and a number of their partners in the public-safety and national-security community. Their main value for PSTP will be largely as an intermediate product.

The next step will be to assess how to use the proceedings to drive the interdepartmental discussions of national security challenges to provide input into the capabilities needed to meet these challenges, and, to define how S&T Foresight and strategic S&T investments in the new Defence R&D Canada Centre for Security Science could help Canada to acquire those capabilities.

For 2006-07, a second round of foresight events, focused on a deeper scanning assessment, and more niche aligned work in cyber security, food security and nano-bio-nano systems technology convergence is being discussed for the January-April 2007 time period.